Los Alamos
NATIONAL LABORATORY
EST. 1943

Acquisition Services Management Division (ASM)
Subcontracts Group
PO Box 1663, Mail Stop P215
Los Alamos, New Mexico 87545
505-665-7888/Fax 505-665-8660

Date: September 26, 2012
Refer To: **191850-1**

Potential Offerors

Salutation: Request for Qualifications

The Los Alamos Nuclear Security, LLC (LANS), a limited liability company which manages and operates Los Alamos National Laboratory (LANL) pursuant to Contract No. DE-AC52-06NA25396 between the U.S. Department of Energy (DOE) / National Nuclear Security Administration (NNSA) and LANS, requires Pre-Employment Background Investigation Services. Los Alamos National Laboratory intends to issue a Request for Proposal (RFP) for a Fixed Unit Price type subcontract to provide Pre-Employment Background Investigation Services in late calendar 2012. The services will include providing domestic criminal history, credit bureau file records, employment history, educational history, military history, driver's license history, sex-offender registry history, and personal references. The services will also require providing international educational history background investigations.

This requirement is an 8(a) Small Business Set Aside. The North American Industry Classification System (NAICS) code 561611 will be utilized for this acquisition. The small business size standard for the listed NAICS code is $12.5M.

A questionnaire consisting of seven (7) pre-qualification questions will be utilized to determine Offerors qualifications. Offerors are encouraged to read the questionnaire in its entirety. Questions in regards to the request for qualifications must be submitted to Vanessa Velarde at vanessav@lanl.gov no later than 3:00 PM Mountain Time, October 4, 2012. Do not submit questions one by one. All questions must be submitted at one time, on one (1) "Word" document. Verbal questions will not be permitted. Answers to all submitted questions will be provided via addendum to this request for qualification. Addendums to this Request for Qualifications will be posted on the LANL website.

The RFP will be sent only to potential Offerors who are deemed qualified to provide the services. To be deemed qualified, a potential Offeror must provide documentation that clearly demonstrates its qualifications to meet each question of the Request for Qualifications identified within Attachment No. 1 titled "Questionnaire".

All information submitted must be organized in a manner that will allow reviewers to easily locate responses to questions. Each question must be answered independently and in sequence as identified on the questionnaire.

Responses shall not exceed two (2) pages per question utilizing Arial 12 font. Responses shall to be provided in original and two (2) copies, to the undersigned not later than 2:00 PM Mountain Time on October 30, 2012.

Information submitted must directly address the Request for Qualifications questions or it may not be considered. Failure to clearly demonstrate qualifications or failure to respond by the due date will result in a potential Offeror not receiving the RFP.

Attachment No. 2 titled "Offeror's Certification Statement" must be signed dated and made a part of the response package.

Proposal submissions sent via the U. S. Postal Service should be addressed as follows:

Los Alamos National Security, LLC
Attn: Vanessa Velarde
P.O. Box 1663, MS P215
Los Alamos, New Mexico 87545

Proposal submissions sent via other delivery services such as UPS, Federal Express, Airborne, etc. should be addressed as follows:

Los Alamos National Security, LLC
Attn: Vanessa Velarde, MS P215
Bldg. SM-30 Bikini Atoll Road
Los Alamos, New Mexico 87545

Proposals that are hand-carried should only be delivered to:

Los Alamos National Security, LLC
Attn: Vanessa Velarde
125 Central Park Square (Across 15th Street from the YMCA)
Los Alamos, New Mexico 87544

Regards,

Vanessa Velarde

Vanessa Velarde
Procurement Specialist

Enclosures: Attachment No. 1, Questionnaire
Attachment No. 2, Offeror's Certification Statement
Attachment No. 3, LANS Policy P204.1

Request for Qualifications
Attachment No. 1
Questionnaire

1.	Does Offeror have a minimum of 5 years of Federal Government pre-employment investigation business experience including international experience? NOTE: Offeror must provided documentation clearly demonstrating number of years conducting business within the Federal Government pre-employment investigation industry.
2.	Does Offeror have experience with Federal Government organizations that request an average of 1,200 pre employment investigations per year? NOTE: Offeror must provide name of agencies and average investigations conducted per year.
3.	Can Offeror provide investigative information to include domestic criminal history, credit bureau file records, employment history, educational history, military history, driver's license history, sex-offender registry history, and personal references? NOTE: Offeror must provide a document demonstrating how the information is reported, including international request.
4.	Can Offeror protect Personally Identifiable Information (PII) according to LANS policy P204.1? NOTE: Offeror must provide documents demonstrating how they will protect PII.
5.	Can Offeror retrieve information by date of birth and social security number? NOTE: Offeror must provide documents demonstrating how they will retrieve information by date of birth and social security numbers.
6.	Can Offeror meet a 7 day deadline for high priority request and a 10 day deliverable for regular requests? NOTE: Offeror must provide documents demonstrating how they will meet LANS 7 day deadline for high priority request.
7.	Does the Offeror use OS XP or Windows 7 or above operation systems in its business environment? NOTE: Offeror must provide a written documentation describing its computer operations environment and capabilities in using the requisite computer operating system.

Request for Qualifications
Attachment No. 2
Offeror's Certification Statement

Qualifying submission packages must be accompanied by the following statement, signed and dated by a company officer of the prime Offeror or other company official having the authority to make such a certification:

The undersigned certifies that the information and qualifications set forth herein are true and correct and may be used as a basis for qualifying for the LANS Pre-Employment Background Investigation Services Request for Proposal (RFP) No. 191850-1.

Preparer: _____

Signature: _____

Title: _____

Date: _____

Please provide the following information as part of the Offeror's Certification Statement.

Company Name	
Mailing Address	
Point of Contact	
Email Address	
Phone	

No: P204-1
Revision: 3

Issued: 03/02/12
Effective Date: 03/02/12

Controlled Unclassified Information

1.0 PURPOSE

The purpose of this document is to present requirements and procedures for identifying, marking, handling, and protecting information that while not classified, falls under one or more categories of information that requires protection from unauthorized dissemination.

2.0 AUTHORITY AND APPLICABILITY

2.1 Authority

This document is issued under the authority of the Laboratory Director to direct the management and operation of the Laboratory, as delegated to the Associate Director for Security and Safeguards (ADSS) as provided in the Prime Contract. This document derives from the Laboratory Governing Policies, particularly the section on Safeguards and Security.

- Issuing Authority (IA): Associate Director for Security and Safeguards (ADSS)
- Responsible Manager (RM): Safeguards (SAFE) Division Leader
- Responsible Office (RO): Classification Group (SAFE-1)

2.2 Applicability

This document applies to all Laboratory workers responsible for Controlled Unclassified Information (CUI) in any location.

3.0 PROCEDURE DESCRIPTION

Requirements for different kinds of CUI are derived from different sources. The requirements for accessing, storing, marking, reproducing, receiving, transmitting, and destroying different types of CUI vary according to the directives from which the requirements are derived.

The requirements for each category of CUI can be found in the sections of this document as follows:

- Section 3.3: Accessing
- Section 3.4: Storing
- Section 3.5: Marking
- Section 3.6: Reproducing
- Section 3.7: Receiving and Transmitting
- Section 3.8: Destroying

3.1 Types of Controlled Unclassified Information (CUI)

CUI consists of the categories of information listed below.

- Official Use Only (OUO), which includes Personal Identifiable Information (PII), Export Controlled Information (ECI) and Applied Technology (AT)
- Naval Nuclear Propulsion Information (NNPI)
- Reactor Safeguards Information (RSI)
- Unclassified Controlled Nuclear Information (UCNI)
- Los Alamos National Security, LLC (LANS) Contractor Owned and Proprietary Information (LPI)

3.2 Identifying Controlled Unclassified Information (CUI)

The following criteria will help identify which categories of CUI, if any, apply to a document under review, assuming it is not classified.

Each document that may contain CUI must be evaluated against all of the following criteria. The information in the document must be evaluated against the criteria for every category; a document may contain information from several categories of CUI. A distinction must also be made between Department of Energy (DOE) and non-DOE information. If, for example, a report is produced in a Department of Homeland Security (DHS) funded project, the document should be marked according to DHS marking guidelines. If information fits more than one category, contact SAFE-1 for further guidance.

3.2.1 Classification

If the document contains information that may be classified, then it must be reviewed by a Derivative Classifier (DC).

3.2.2 Official Use Only (OUO)

3.2.2.a Mandatory Determination

Some kinds of information are designated as OUO by an approved DOE classification guide or other guidance document. Materials that meet these criteria are always subject to OUO requirements. This process of identifying OUO is called "mandatory determination."

Note: OUO identified by mandatory determination should be the result of a DC review.

3.2.2.b Discretionary Determination

Other information is designated as OUO because it meets certain criteria that may make it eligible for denial of release under the Freedom of Information Act (FOIA). The worker or manager responsible for the material being considered for OUO protection determines whether the material meets the OUO criteria. This process of identifying OUO is called "discretionary determination."

Discretionary determinations should be made by considering programmatic information protection requirements. Program Managers should create and distribute guidelines for their programs containing instructions on the type of information that should be protected as OUO.

Materials must meet all of the following three criteria in order to allow a discretionary determination as OUO:

- The information must be government owned information.
- The worker responsible for the information must determine that the information has the potential to damage governmental, commercial, or private interests if disseminated to persons who do not need the information to perform DOE-authorized activities.
- The worker responsible for the information must determine that it relates to any of the seven FOIA exemptions shown in Section 3.2.2.c.

The original (record copy) of documents identified as containing OUO information through a discretionary determination must have a cover sheet that explains the following:

- what information in the document is considered OUO,
- how release of the information would have the potential to damage governmental, commercial, or private interests, including possible consequences of release, and
- why the information fits into the chosen FOIA category.

If submitted to SAFE-1 for release as a Los Alamos-Controlled Publication (LA-CP), the submission package must include a copy of this cover sheet. (See Section 12 for the list of LA-CP Forms.)

3.2.2.c Freedom of Information Act (FOIA) Exemptions for Official Use Only (OUO)

Exemption 3—Statutory Exemption: Protects information whose disclosure is specifically prohibited by law, e.g., the Federal Transfer Technology Act allows Federal agencies to protect for five years any commercial and business confidential information that results from a Cooperative Research and Development Agreement (CRADA) with a non-Federal party.

Exemption 4—Commercial/Proprietary: Protects trade secrets or confidential business information, e.g., details of a unique manufacturing process, or research data generated by a private corporation.

Exemption 5—Privileged Information

- Deliberative Process: Protects the government's decision-making process, e.g., comments on options for a project or about joint decisions yet to be made.
- Attorney Work-Product Privilege: Protects documents and other correspondence prepared by an attorney in contemplation of litigation.
- Attorney-Client Privilege: Protects confidential communications between an attorney and his or her client.

Exemption 6—Personal Privacy: Protects information that could cause the individual involved personal distress or embarrassment, e.g., personnel records, health records, or security records.

Exemption 7—Law Enforcement: Protects information compiled for enforcing civil, criminal, or military law, e.g., details of an active law enforcement investigation, information that could reveal the identity of a confidential source, or information that could reasonably be expected to endanger someone's life or physical safety.

Exemption 8—Financial Institutions: Protects information for the use of any agency responsible for the regulation or supervision of financial institutions.

Exemption 9—Wells: Protects information concerning geological and geophysical information and data, including maps, concerning wells.

Note 1: Exemptions 8 and 9 are rarely used and generally not applicable at the Laboratory.

Note 2: The person making the OUO determination is responsible for selecting the appropriate exemption.

An unclassified document that contains both UCNI and OUO must be marked with both markings and handled as required for UCNI, which is the more restrictive handling requirement.

Government-owned documents containing PII, ECI or AT information are OUO and must be marked according to the requirements for OUO. In addition to the standard OUO markings, these documents should be marked as containing PII, ECI or AT, as appropriate. See Section 3.5.1 for marking requirements.

Note: Contractor-owned documents must not be marked OUO. See Section 3.2.3.

3.2.2.d Personal Identifiable Information (PII)

PII is a type of OUO that falls under FOIA Exemption 6, Personal Privacy.

PII is any information collected or maintained by the DOE or its contractor organizations about an individual, including but not limited to financial transactions, medical history and criminal or employment history, and information that can be used to distinguish or trace an individual's identity, such as his/her name, Social Security Number (SSN), date and place of birth, mother's maiden name, biometric data, and including any other personal information that is linked or linkable to a specific individual.

Examples of PII:

- SSNs in any form.
- Place of birth associated with an individual.
- Date of birth associated with an individual.
- Mother's maiden name associated with an individual.
- Biometric records associated with an individual, such as fingerprints, iris scans, or DNA information.
- Medical history information associated with an individual, such as previous diseases, metric information, weight, height, and blood pressure.
- Criminal history associated with an individual.
- Employment history associated with an individual, such as ratings, and disciplinary actions.
- Financial information associated with an individual, such as credit card numbers and bank account numbers.
- Security clearance history or related information.

What is not PII:

- Phone numbers (work, home, cell).
- Street addresses (home, work, other).
- E-mail addresses (work or personal).
- Digital pictures.
- Birthday cards.
- Birthday e-mails.
- Grade and step information for federal employees.
- Medical information pertaining to work status (X is out sick today).
- Medical information included in a health or safety report (X broke his arm when…).
- Resumes (unless they include SSNs).
- Job titles for employment history, resume, or written biography.
- Federal salaries.
- Written biographies, such as the ones used in pamphlets of speakers.
- Alma Mater or degree level in biographies.
- Personal information stored by individuals on their personal workstation or laptop (unless it includes an SSN).
- Z numbers

3.2.2.e Export Controlled Information (ECI)

ECI is a type of OUO dealing with unclassified technology information, the export of which is controlled by the provisions of the Department of Commerce Export Administration Regulations, the Department of State International Traffic in Arms Regulations, or other United States (US) export control statutes and/or regulations.

Note: Contact the Export Control Team, 665-2194, for more information about ECI.

3.2.2.f Applied Technology (AT)

AT is a type of OUO dealing with unclassified information determined by the DOE to describe certain scientific and technical information related to engineering, development, design, construction, operation, or technology advances in projects or facilities that have received major funding emphasis.

Note: AT information at the Laboratory will be clearly identified as such by the Department of Energy Office of Nuclear Energy (DOE-NE). Laboratory workers are not responsible for evaluating information for designation as AT. SAFE-1 can provide additional assistance concerning AT information.

3.2.3 *Los Alamos National Security, LLC (LANS) Contractor Owned and Proprietary Information (LPI)*

The LANS/National Nuclear Security Administration (NNSA) Prime Contract identifies the ownership of records created or maintained in the performance of the contract. Those records are either Government-owned records or LANS-owned records. The large majority of scientific, technical and operational records are owned by the Government. However, a relatively small but significant body of records is owned and therefore primarily controlled by LANS. The types of records that are owned by LANS generally fall within these categories:

- Employment, medical, and legal
- LANS financial, and corporate information
- Licensing, technology transfer, and CRADA
- Procurement

Note 1: Documents containing LPI should not be marked "Official Use Only" or "OUO" unless they also contain information that meets the exemption criteria for OUO. Markings to designate as LPI are discretionary, not mandatory. The determination to mark such documents should be made by the owner of the information and based upon programmatic sensitivities.

Note 2: Although marking LPI is optional, the term LPI must be used instead of "business sensitive." Business sensitive is not a defined term and is therefore not a recognized category of information at LANL. LPI includes any information relating to the business, operations, and programs of LANS not generally known by persons not employed by LANS. This includes technology transfer documents such as license agreements, including appendices containing royalty rates or information, financial information, commercialization plans and related notes, documents and correspondence, nondisclosure agreements, and CRADA information.

3.2.3.a Employment Information

Employment sensitive information may include personnel records, salary (including payroll information), employee benefits information, drug testing records, labor negotiation records, workers compensation records, medical/health related records, Employee Assistance Program records, employment/disciplinary investigation records, ethics records, and employee concerns.

3.2.3.b Procurement Information

Procurement sensitive information may include any documentation relating to a potential or actual procurement, including purchase requests, statements of work, specifications, purchase orders, subcontracts, proposals, technical evaluation criteria, and documentation related to source selection, bid, evaluation, and award of LANS subcontracts.

Exclusion: This guidance does not apply to information that is protected by a legal privilege such as the attorney-client privilege. Such information should be labeled as directed by LANS counsel.

3.2.4 *Reactor Safeguards Information (RSI)*

Documents may be designated RSI if they contain:

- unclassified information related to nuclear power reactors,
- information about postulated threats and security measures for Special Nuclear Material (SNM), and/or

- the location and security measures for certain plant equipment vital to the safety of production or utilization facilities associated with power reactors or other facilities under Nuclear Regulatory Commission (NRC) control.

Note: RSI does not apply to DOE facilities. RSI content for NRC-licensed facilities is very similar in nature to content designated as UCNI, which applies to security-related information about DOE facilities. (Specific controls for RSI and UCNI differ, as documented below.)

3.2.5 Naval Nuclear Propulsion Information (NNPI)

Documents may be designated unclassified NNPI if they contain unclassified information concerning any aspect of the propulsion plants of naval nuclear-powered ships and prototypes, including their associated nuclear support facilities. Some NNPI is classified. Unclassified NNPI is considered CUI.

Note: Guidance for NNPI is provided by NA-30, the DOE Naval Nuclear Office.

3.2.6 Unclassified Controlled Nuclear Information (UCNI)

Documents may be designated UCNI if they contain:

- unclassified information concerning facilities that produce or utilize nuclear material, or
- security information about such facilities (other than Naval Nuclear Propulsion systems), or
- information previously classified as Restricted Data (RD) that has been declassified, and whose unauthorized dissemination could be reasonably expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of illegal production of nuclear weapons, or theft, diversion, or sabotage of nuclear materials, equipment, or facilities.

Documents that may contain UCNI must be reviewed by an UCNI Reviewing Official.

3.3 Access to Controlled Unclassified Information (CUI)

3.3.1 Need to Know

Any worker who has been granted access to matter containing CUI **must** determine another worker's need-to-know before granting access to that matter.

Need-to-know **must** be established by

- determining what matter will be accessed, and
- determining that the recipient requires access to the matter to perform his or her official duties through
  - current relationships, tasks, duties, and assignments, or
  - confirmation by an RLM.

Incidental access may be granted to individuals who handle or come into contact with classified matter (such as LANL employees or external organizations performing audits), but whose job functions do not include review or other use of the classified matter.

Note: The person having responsibility for the information determines need-to-know. In some cases (such as audits by external organizations), need-to-know may be determined by LANL senior management or other government agency rather than the person responsible for the information.

3.3.2 Access Requirements for Official Use Only (OUO)

Access to (a) documents marked as containing OUO information and, (b) OUO information from such documents must only be provided to those persons who have a need to know.

If the information is OUO because it is ECI, access is restricted to US persons (citizens and Lawful Permanent Residents), and to those others authorized according to US export control regulations. Therefore, such information may not be publicly released. Often, such information is proprietary in nature.

If the information is OUO because it is AT, it is subject to access restrictions established by the DOE program office. The program manager responsible for the AT information can assist workers in determining access authorization for Laboratory workers.

3.3.3 Access Requirements for Naval Nuclear Propulsion Information (NNPI)

Access to NNPI must be granted only to US citizens who have a need to know.

3.3.4 Access Requirements for Reactor Safeguards Information (RSI)

RSI material is subject to access restrictions established by the NRC. The Laboratory program manager responsible for the RSI information can assist workers in determining access authorization for Laboratory workers.

3.3.5 Access Requirements for Unclassified Controlled Nuclear Information (UCNI)

No security clearance is required for access to UCNI.

UCNI documents or information must be provided only to those who have a need to know the specific UCNI in the performance of official duties or of DOE-authorized activities.

UCNI documents or information must be provided only to those authorized for routine or special access as explained below.

Any individual who has routine access to UCNI must grant routine access to specific UCNI to any other individual only after determining that the person to whom they are granting access has a need to know the specific information in question.

3.3.5.a Routine Access

To be authorized for routine access to UCNI, an individual must be one of the following:

- a federal employee or member of the US Armed Forces (whether or not a US citizen),
- an employee of a federal contractor or subcontractor (whether or not a US citizen),
- a federal consultant or DOE advisory committee member (whether or not a US citizen), or
- a US citizen who is also one of the following:
  - an employee of a prospective federal contractor or subcontractor who will use the UCNI for the purpose of bidding on a federal contract or subcontract,

- a member of Congress or a staff member of a congressional committee or of an individual member of Congress,
- the governor of a state, his/her designated representative, or a state government official; a local government official or a Native American tribal government official, or
- a member of a state, local, or Native American tribal law enforcement or emergency response organization,

▪ someone other than a US citizen, who requires routine access to specific UCNI in conjunction with one of the following:

Note: The Authorized Individual who desires to release UCNI to a person for the reasons listed in this section must coordinate such release with the DOE Secretarial Officer or NNSA Deputy Administrator or Chief with cognizance over the information. (For example, release of security-related UCNI at any site requires the approval of the Director of Safeguards and Security, not the program office that manages the site.)

- an international nuclear cooperative activity approved by the US Government,
- US diplomatic dealings with foreign government officials,
- an agreement for cooperation under Section 123 of the Atomic Energy Act, or
- provisions of treaties, mutual defense acts, or federal contracts or subcontracts.

Note: The DOE Office of Safeguards and Security may approve a waiver or recommend approval of an exception for access to UCNI by individuals who do not otherwise meet the access requirements.

3.3.5.b Special Access

Special access may be granted to individuals not authorized for routine access to UCNI. For example, special access might be granted to an attorney representing an employee in litigation with DOE.

A request for special access to UCNI may be submitted through the cognizant DOE or NNSA security office to the cognizant DOE Secretarial Officer or NNSA Deputy Administrator or Chief.

The request must include: a) the intended recipient's name, current residence or business address, birthplace, birth date, and country of citizenship; b) a description of the UCNI requested; c) a description of the purpose for which the UCNI is needed; and d) certification by the intended recipient of his/her understanding of, and willingness to abide by, the requirements in 10 Code of Federal Regulations (CFR) 1017, *Identification and Protection of Unclassified Controlled Nuclear Information*.

Note: A related group of individuals may be eligible for approval for special access to UCNI. In such a case, the relationship of the individuals must be described, but the individuals themselves need not be identified. (Example: All attorneys and paralegals of a law firm who are representing a client in a lawsuit against a DOE site.) Requests for such categorical special access approval are submitted to the DOE Director of Safeguards and Security.

Within 30 days of the receipt of the request, the cognizant DOE Secretarial Officer or NNSA Deputy Administrator or Chief must notify the requester of the determination, or, if a determination cannot be made within 30 days, the date when the determination will be made.

Note: A person granted special access to specific UCNI is not an Authorized Individual and must not further disseminate the UCNI.

Each person granted special access to UCNI must be notified of applicable regulations concerning UCNI before dissemination of the UCNI.

3.3.6 Access Requirements for Los Alamos National Security, LLC (LANS) Contractor Owned and Proprietary Information (LPI)

Access to LPI should only be given to LANS employees or private third-parties such as consultants, subcontractors or other Management and Operating (M&O) contractors with a need to know. LPI may be provided to the NNSA customer on a specific request basis with approval from the RLM who owns the information.

3.4 Storing Controlled Unclassified Information (CUI)

3.4.1 Official Use Only (OUO) Including Personal Identifiable Information (PII), Export Controlled Information (ECI) and Applied Technology (AT)

Documents and Removable Media

Workers must take reasonable precautions to prevent unauthorized access to OUO information, such as storing it in a locked room or locked receptacle (e.g., locked file cabinet, desk, bookcase, or briefcase).

OUO material may be stored without additional protections in a building where internal security is provided during nonwork hours (e.g., presence of Protective Force patrols, location in a limited area).

Electronic Files

To prevent unauthorized access, OUO information stored on a computer must be protected by one or more of the following controls: passwords, authentication, encryption, or file access control.

Note: Storing OUO files on a LANL computer will satisfy the protection requirements. On a non-LANL computer, the owner must ensure OUO files are protected from unauthorized access.

3.4.2 Los Alamos National Security, LLC (LANS) Contractor Owned and Proprietary Information (LPI)

Documents and Removable Media

Workers must take reasonable precautions to prevent unauthorized access to LPI, such as storing it in a locked room or locked receptacle (e.g., locked file cabinet, desk, bookcase, or briefcase).

Material containing LPI may be stored without additional protections in a building where internal security is provided during nonwork hours (e.g., presence of Protective Force patrols, location in a limited area).

Electronic Files

To prevent unauthorized access, LPI stored on a computer must be protected by one or more of the following controls: passwords, authentication, encryption, or file access control.

Note: Storing LPI files on a LANL computer will satisfy the protection requirements. On a non-LANL computer, the owner must ensure LPI files are protected from unauthorized access.

3.4.3 Naval Nuclear Propulsion Information (NNPI)

Documents and Removable Media

Unclassified NNPI must be protected in accordance with Naval Sea Systems Command Instruction (NAVSEAINST) C5511.32B, *Safeguarding of Naval Nuclear Propulsion Information (NNPI) Naval Sea Systems Command Instruction*. NNPI must be protected pursuant to export control requirements and statutes.

Note: Contact The Classification Office for more information.

Electronic Files

To prevent unauthorized access, NNPI stored on a computer must be protected by one or more of the following controls: passwords, authentication, encryption, or file access control.

Note: Storing NNPI files on a LANL computer will satisfy the protection requirements. On a non-LANL computer, the owner must ensure NNPI files are protected from unauthorized access.

3.4.4 Reactor Safeguards Information (RSI)

Documents and Removable Media

RSI material must be protected in a locked General Services Administration (GSA)-approved repository when unattended.

Knowledge of lock combinations for such containers should be limited to a minimum number of personnel for operating purposes, who are otherwise authorized to access the information.

Electronic Files

To prevent unauthorized access, RSI stored on a computer must be protected by one or more of the following controls: passwords, authentication, encryption, or file access control.

Note: Storing RSI files on a LANL computer will satisfy the protection requirements. On a non-LANL computer, the owner must ensure RSI files are protected from unauthorized access.

3.4.5 Unclassified Controlled Nuclear Information (UCNI)

Documents and Removable Media

When UCNI is in use, the user must maintain physical control over the material to prevent unauthorized access to the information.

When it is not in use, UCNI matter must be stored in a locked room or locked receptacle (e.g., locked file cabinet, desk, bookcase, or briefcase), or, if in secured areas or facilities, in a manner that would prevent inadvertent access by an unauthorized individual. The locked room or receptacle must have controls that limit access only to authorized individuals.

Note: Administrative (Level IV) locks and keys are sufficient to protect UCNI. See P202-4, *Security Locks and Keys*, for more information on Level IV locks and keys.

Electronic Files

To prevent unauthorized access, UCNI stored on a computer must be protected by one or more of the following controls: passwords, authentication, encryption, or file access control.

Note: Storing UCNI files on a LANL computer will satisfy the protection requirements. On a non-LANL computer, the owner must ensure UCNI files are protected from unauthorized access.

3.5 Marking Controlled Unclassified Information (CUI)

3.5.1 Official Use Only (OUO)

Additional markings based on laws, regulations, or other DOE directives that convey additional advice on handling or access restrictions are allowed.

Cover Marking Requirements

The front page of documents containing OUO must be marked with the following information:

OFFICIAL USE ONLY
May be exempt from public release under the Freedom of Information Act
(5 U.S.C §552 [1966]) as amended, exemption and category: _____
_____
_____
_____

Department of Energy review required before public release

Name/org: _____ Date: _____
Guidance (if applicable): _____
_____

"Guidance" refers to the classification guide or other DOE-approved guidance document used to make a mandatory OUO determination.

Note: The "guidance" line is not filled in for discretionary OUO determinations.

Additional control or handling markings (controlled distribution notice, CRADA, etc.) may be applied, if appropriate, in addition to, but not in place of the OUO cover marking.

Page Marking Requirements

Each subsequent page must be marked, either on the bottom of each page or on the bottom of only those pages containing OUO information, with the following:

`Official Use Only`

or, if space is limited,

`OUO`

Relationship of Official Use Only (OUO) Markings to Other Types of Control Markings

Unclassified Documents: The OUO front marking must be applied to any unclassified document that contains OUO information regardless of any other unclassified control marking (e.g., UCNI). This means that documents containing both UCNI and OUO information must be marked with both front markings.

OUO Documents that contain PII, ECI or AT should be marked with PII, ECI or AT, as appropriate, in addition to the OUO marking, to clarify the protection requirements for the information.

Classified Documents: OUO front and page markings must not be applied to any classified document that also contains OUO information. However, if the classified document has been portion marked, the acronym "OUO" must be used to indicate those portions containing only OUO information.

Other Marking Requirements

OUO Documents containing ECI should show the following statement on the document's front page or cover sheet in addition to the OUO statement:

```
EXPORT CONTROLLED INFORMATION
This document contains technical data, the export of which is
restricted by the Arms Export Control Act (22 U.S.C. §2751, et
seq.), the Atomic Energy Act of 1954, as amended
(42 U.S.C. §2077), or the Export Administration Act of 1979, as
amended (50 U.S.C. §2401, et seq.). Violations of these laws may
result in severe administrative, civil, or criminal penalties.
```

In addition, the following marking should appear at the bottom of the page on each interior page that contains ECI:

```
EXPORT CONTROLLED INFORMATION
```

OUO documents containing designated AT information must be marked on the front page or cover sheet with the following text in addition to the OUO statement:

```
APPLIED TECHNOLOGY
Any further distribution by any holder of this document or data
therein to third parties representing foreign interests, foreign
governments, foreign companies, and foreign subsidiaries or
foreign divisions of U.S. companies shall be approved by the
(insert appropriate DOE/NE program office official), U.S.
Department of Energy. Further, foreign party release may require
DOE approval pursuant to 10 CFR 810, and/or may be subject to
section 127 of the Atomic Energy Act.
```

Special format information (e.g., photographs, viewgraphs, films, magnetic tapes, floppy diskettes, audiotapes, videotapes, Digital Video Discs [DVDs], or Compact Disc-Read Only Memory [CD-ROMs]) must be marked in a manner consistent with the requirements for marking documents. When space is limited (e.g., 35-mm slide), the page marking is sufficient.

Documents that may contain OUO information that are maintained in restricted access files (e.g., personnel office files) do not need to be marked as long as they remain in the file. If the documents are retrieved from the files, they do not need to be marked as long as the documents will be returned to the files and are not accessible by individuals who are not authorized to access the OUO information. A document (or a copy) removed from restricted access files that will not be returned must be reviewed to determine whether it contains OUO information and, if appropriate, marked.

Transmittal documents that do not contain OUO information themselves but that transmit OUO attachments must be clearly marked on the front page as follows:

```
Document transmitted contains OUO information.
```

Marking Official Use Only (OUO) E-mail

E-mail messages that contain OUO information must indicate OUO in the first line, before the body of the text.

E-mail messages must also indicate when attachments contain OUO information. An e-mail with an OUO attachment is considered a transmittal document.

Note: E-mail subject lines and attachments must not indicate OUO.

Removing Official Use Only (OUO) Markings

In the case of OUO markings applied in accordance with mandatory guidance issued by DOE/NNSA, such markings may only be removed when the applicable guidance specifies that the information is no longer OUO.

When discretionary markings are applied by an employee after consideration of the OUO criteria, such markings may be removed by the employee who made the original determination, or his or her supervisor.

IMPORTANT! From July 18, 1949 to October 22, 1951, the Atomic Energy Commission used the phrase "Official Use Only" as a designation for certain classified information. Documents generated in that time period and marked as OUO must be handled as Confidential-National Security Information until their proper classification is determined by a Derivative Classifier.

3.5.2 *Los Alamos National Security, LLC (LANS) Contractor Owned and Proprietary Information (LPI)*

Material containing LPI should bear the following marking on the front page:

```
LANS XXXXXX-Sensitive Information

Name/org: _____

Date: _____
```

Where XXXXXX is BUSINESS, EMPLOYMENT, or PROCUREMENT. See Section 3.2.3 for descriptions of information falling into each of these categories.

In conjunction with the label described above, instruction should be provided for handling and distribution either above or below the label. Use one of the following, as appropriate:

```
DO NOT COPY OR DISTRIBUTE
```

Use this instruction when the intent is to completely prohibit further distribution. This instruction may be appropriate when a manager is providing information to his or her own employees or to private third parties such as consultants, subcontractors, or other M&O contractors.

```
INTERNAL USE ONLY - DO NOT DISTRIBUTE OUTSIDE OF LANS
```

This instruction is for use when the information is to be shared only with LANS employees. Such documents may be provided to the NNSA customer on a specific request basis.

```
DO NOT DISTRIBUTE WITHOUT THE EXPRESS WRITTEN PERMISSION OF LANS
```

or

```
DO NOT DISTRIBUTE OUTSIDE OF THE NNSA WITHOUT
EXPRESS WRITTEN PERMISSION OF LANS
```

This instruction is intended for use when providing information to the NNSA customer, but when there is a need to control additional distribution.

LPI Documents that contain PII or ECI should add /PII or /ECI, as appropriate, in addition to the LPI marking to clarify the protection requirements for the information.

Page Marking Requirements

Each subsequent page must be marked, either on the bottom of each page or on the bottom of only those pages containing LPI, with the following:

```
LANS XXXXXX-SENSITIVE INFORMATION
```

Where XXXXXX is BUSINESS, EMPLOYMENT, or PROCUREMENT.

Or, if space is limited,

```
LPI
```

Marking Los Alamos National Security, LLC (LANS) Contractor Owned and Proprietary Information (LPI) E-mail

E-mail messages that contain LPI must indicate LPI in the first line, before the body of the text.

E-mail messages must also indicate when attachments contain LPI. An e-mail with an LPI attachment is considered a transmittal document.

Note: E-mail subject lines and attachments must not indicate LPI.

3.5.3 *Naval Nuclear Propulsion Information (NNPI)*

Unclassified and classified NNPI must be marked as not releasable to foreign nationals on the cover page with the following:

```
NOFORN: This document is subject to special export controls, and
each transmittal to foreign governments or foreign nationals may be
made only with the prior approval of the U.S. DOE.
```

The top and bottom of all subsequent pages must be marked:

```
NOFORN
```

Note: NOFORN is an intelligence caveat. The use of NOFORN for NNPI is the only situation in which intelligence caveats may be used for marking documents that are not intelligence related.

3.5.4 *Reactor Safeguards Information (RSI)*

Documents containing RSI must be conspicuously marked "Safeguards Information" (e.g., on the top and bottom of each page, including the cover) to indicate the presence of protected information.

RSI must not be marked as classified or as UCNI.

3.5.5 *Unclassified Controlled Nuclear Information (UCNI)*

UCNI markings must be applied to any unclassified matter that contains UCNI, even if it already has other unclassified control markings (e.g., OUO). These marking requirements apply to electronic and paper documents.

Page Marking Requirements

UCNI documents must be marked on the bottom of every page or on the bottom of those pages that contain UCNI with the following:

```
Unclassified Controlled Nuclear Information
```

or

```
UCNI
```

Cover Marking Requirements

The following statements must be added to the cover of the document:

Reviewing Official: _____ (Name/Organization) Date: _____ Guidance Used: _____ _____ (List all UCNI guidance used)	UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION NOT FOR PUBLIC DISSEMINATION Unauthorized dissemination subject to civil and criminal sanctions under section 148 of the Atomic Energy Act of 1954, as amended (42 U.S.C. §2168 [2008]).

Special Format Marking Requirements

Special formats of unclassified matter (photographs, viewgraphs, films, magnetic tapes, floppy disks, audio or videotapes, or slides) must be marked to the extent practical as described above so that users can easily recognize UCNI material.

Unclassified fixed and removable computer media that contain UCNI must be marked with the legend:

UCNI

Portion Marking Requirements

UCNI markings must not be applied to a classified document that contains UCNI unless the document requires portion marking.

If a classified document does require portion marking, each unclassified portion that contains UCNI must be identified and marked.

Note: See P204-2, *Classified Matter Protection and Control Handbook*, for full requirements on portion marking classified documents.

Marking UCNI E-mail

E-mail messages that contain UCNI must indicate UCNI in the first line, before the body of the text.

E-mail messages must also indicate when attachments contain UCNI. An e-mail with an UCNI attachment is considered a transmittal document.

Note: E-mail subject lines and attachments must not indicate UCNI.

3.6 Reproducing Controlled Unclassified Information (CUI)

All CUI information must be reproduced only to the minimum extent necessary to carry out official activities.

3.6.1 Official Use Only (OUO)

OUO must be reproduced to the minimum extent necessary to carry out official activities.

Reproduced copies of documents or media that contain OUO must be marked and protected in the same manner as is required for the original.

Copy machine malfunctions occurring while OUO documents are being reproduced must be cleared and all paper paths checked for OUO material. Excess paper containing OUO must be destroyed as described in Section 3.8.

3.6.2 Los Alamos National Security, LLC (LANS) Contractor Owned and Proprietary Information (LPI)

LPI must be reproduced to the minimum extent necessary to carry out official activities, in accordance with the distribution limitation statement on the front page of the document.

Reproduced copies of documents or media that contain LPI must be marked and protected in the same manner as is required for the original.

Copy machine malfunctions occurring while LPI documents are being reproduced must be cleared and all paper paths checked for LPI material. Excess paper containing LPI must be destroyed as described in Section 3.8.

3.6.3 Unclassified Controlled Nuclear Information (UCNI)

The permission of the originator is not required to reproduce matter that contains UCNI.

Reproduced copies of documents or media that contain UCNI must be marked and protected in the same manner as is required for the original.

Copy machine malfunctions occurring while UCNI documents are being reproduced must be cleared with all paper paths checked for UCNI material. Excess paper containing UCNI must be destroyed as described in Section 3.8.

3.7 Receiving and Transmitting Controlled Unclassified Information (CUI)

3.7.1 Official Use Only (OUO)

Los Alamos National Laboratory (LANL) Interoffice Mail

OUO material that is transmitted within LANL using the internal mail system must be placed inside a sealed, opaque envelope with the recipient's address and the words TO BE OPENED BY ADDRESSEE ONLY on the front.

Note: Government-owned documents containing PII and ECI are OUO and must follow receiving and transmitting requirements for OUO. In addition to the standard OUO markings, these documents should be marked as containing PII or ECI, as appropriate.

Mail Outside the Laboratory

OUO material transmitted outside LANL must be placed inside a sealed, opaque envelope or wrapping, marked with the recipient's address, a return address, and the words TO BE OPENED BY ADDRESSEE ONLY.

OUO documents containing AT matter must be sent with transmittal sheets marked to indicate that the document being transmitted contains AT information. The following language (or its equivalent) must be used:

```
"The attachment contains applied technology information
requiring conformance to U.S. Department of Energy program
policy and the Applied Technology legend." (DOE G 241.1-1)
```

Any of the following US mail delivery categories may be used: first class, express, certified, or registered mail.

Any commercial carrier may be used.

Hand-Carrying Between Sites, Within a Site, or Off Site

OUO information may be hand-carried between sites, within a site, or off site as long as the worker carrying the information can meet all requirements for protecting and controlling access to the material.

Fax and Other Telecommunications Circuits

OUO information should be protected by encryption whenever possible when it is transmitted over telecommunications circuits.

When using an unencrypted fax, transmission must be preceded by a telephone call to the recipient so that the document can be controlled when it is received.

If encryption capabilities are not available and transmission by mail is not a feasible alternative, then regular facsimile machines may be used to transmit the document.

E-mail and Electronic Transmission

When OUO information is sent over networks, including e-mail, encryption is not required but it is highly encouraged. Alternatively, OUO documents may be sent as password-protected attachments and the recipient called with the password.

If encryption capabilities are not available and transmission by mail is not a feasible alternative, then unencrypted e-mail may be used to transmit the OUO document.

When transmitted electronically outside LANL, OUO documents containing AT must be encrypted with National Institute of Standards and Technology (NIST)-validated encryption software. When transmitted within the LANL yellow network, no encryption is required but it is suggested.

3.7.2 Los Alamos National Security, LLC (LANS) Contractor Owned and Proprietary Information (LPI)

The requirements for receiving and transmitting LPI are identical to the requirements for OUO.

3.7.3 *Naval Nuclear Propulsion Information (NNPI)*

Los Alamos National Laboratory (LANL) Interoffice Mail

The standard interoffice envelope is sufficient.

Outside the Laboratory

NNPI material transmitted outside the Laboratory must be placed in a sealed, opaque envelope or wrapping marked with the recipient's address, a return address, and the words TO BE OPENED BY ADDRESSEE ONLY. Mail may be sent first class, registered, certified, or express service. Any commercial carrier may be used.

Fax

Notify the intended recipient before transmitting the document.

Hand-Carrying Between Sites, Within a Site, or Off Site

NNPI may be hand-carried between sites, within a site, or off site as long as the person carrying the information can control access to the information.

E-mail

When transmitted electronically outside LANL, NNPI must be encrypted with NIST-validated encryption software. When transmitted within the LANL yellow network, no encryption is required but it is suggested.

3.7.4 *Reactor Safeguards Information (RSI)*

Los Alamos National Laboratory (LANL) Interoffice Mail

The standard interoffice envelope is sufficient.

Outside the Laboratory

Documents or other matter, when transmitted outside an authorized place of use or storage, must be packaged so that the presence of protected information is not revealed.

Fax

Except under emergency or extraordinary conditions, RSI must be transmitted only by protected telecommunications circuits approved by the NRC.

E-mail

When transmitted electronically outside LANL, RSI must be encrypted with NIST-validated encryption software (such as Entrust).

When RSI is transmitted within the LANL yellow network, no encryption is required but it is suggested. It is the sender's responsibility to ensure that the recipient understands the sensitivity of the information and the requirements for protecting that information.

3.7.5 *Unclassified Controlled Nuclear Information (UCNI)*

Hand-Carrying Between Sites, Within a Site, or Off Site

UCNI may be hand-carried between sites, within a site, or off site as long as the person carrying the information can control access to the information.

Los Alamos National Laboratory (LANL) Interoffice Mail

The standard interoffice envelope is sufficient.

The envelope must not be marked to indicate that the content within is UCNI.

Outside the Laboratory

An opaque envelope must be used when transmitting UCNI outside the Laboratory.

Outer packaging must not indicate that the content within is UCNI.

UCNI can be mailed using any of the following US mail methods: US First Class, Express, Certified Mail or Registered Mail. Any commercial carrier may be used.

Transmittal Documents

If a transmittal document does not contain UCNI, mark the front of the transmittal document as follows:

```
Matter transmitted contains Unclassified Controlled Nuclear
Information. When separated from enclosures, this document is
not UCNI.
```

If a transmittal document contains UCNI, the transmittal document must be marked as an UCNI document. The document originator must obtain all reviews and approvals required for an UCNI document.

The front of the transmittal document must be marked with the following statement:

```
Matter transmitted contains Unclassified Controlled Nuclear
Information. When separated from enclosures, this document is
UCNI.
```

Telecommunications

In accordance with 10 CFR 1017, *Identification and Protection of Unclassified Controlled Nuclear Information,* as set forth in DOE Order (O) 471.1B, *Identification and Protection of Unclassified Controlled Nuclear Information*, when transmitting UCNI documents over a telecommunications circuit (including the telephone, facsimile, radio, e-mail, Internet), encryption algorithms that comply with all applicable Federal laws, regulations, and standards for the protection of controlled unclassified information must be used. Examples of compliance with this requirement include:

Telephone

Unencrypted voice transmission of UCNI over open phone lines is prohibited. A Secure Terminal Equipment (STE) line is required. All cellular devices must be turned completely off when in proximity to UCNI discussions. Proximity means the voice transmission can be heard by persons nearby.

Fax

UCNI documents must be transmitted using a fax machine that employs encryption.

E-mail

When transmitted electronically outside LANL, UCNI must be encrypted with NIST-validated encryption software. E-mails with UCNI attachments are considered transmittal documents and must be marked as such.

When UCNI is transmitted within the LANL yellow network, no encryption is required but it is suggested. It is the sender's responsibility to ensure that the recipient understands the sensitivity of the information and the requirements for protecting that information.

3.8 Destroying Controlled Unclassified Information (CUI)

The decision to destroy documents or media, whether or not they contain CUI, must be consistent with the policies and procedures for records disposition.

3.8.1 General Requirements

All nonelectronic CUI documents must be destroyed by any means that prevents the retrieval or export of the information.

Workers should destroy CUI material by

- shredding in an approved shredder (see Section 3.8.3 for details), or
- using a burn box approved for unclassified matter.

Note: Other methods may be used to destroy CUI material if they are reviewed and approved by a Subject Matter Expert (SME). Workers must contact their deployed security officers if alternative destruction methods are needed.

3.8.2 Using Burn Boxes to Destroy Controlled Unclassified Information (CUI)

Workers may use burn boxes to dispose of CUI materials including paper, transparencies, film, Mylar, microfiche, floppy disks, and plastic CDs.

Workers must use only official burn boxes (marked "sensitive unclassified data"). No other box will be accepted by the pick up crew.

All paper clips, metal fasteners, and metal binders must be removed from material placed in burn boxes.

3.8.2.a Ordering Burn Boxes

To order official unclassified burn boxes workers must

- e-mail a request to burn-it@lanl.gov, or
- place an order in i-Procurement through a Deployed Procurement Representative.

Note: Unclassified burn boxes are part number SOS16120.

3.8.2.b Preparing the Burn Box

The worker preparing the burn box must:

- Fill the box only two-thirds full.
- Seal all the seams on the box with tape. Clear packaging tape may be used.
- Mark each box with his or her name, telephone number, group, mail stop, location (technical area, building, room), and "Box X of X."
- Complete Form 1704, *Certificate of Records Destruction (Unclassified and Classified)* (for record copies or items of historical value).
- Include a self-addressed return envelope to receive a copy of the destruction record.
- Send an e-mail to burn-it@lanl.gov including his or her name, telephone number, group, mail stop, location (technical area, building, room) and the number of boxes to be destroyed.

Note: The Burn-it Custodian will respond with the estimated pick-up information.

Filled burn boxes waiting for pick-up must be stored in a locked room.

3.8.3 *Shredding Controlled Unclassified Information (CUI) Documents*

A strip-cut shredder that produces strips no more than ¼-inch wide is sufficient for all CUI documents except UCNI.

UCNI documents must be shredded using a cross-cut shredder that produces particles no larger than ¼-inch wide and 2 inches long.

Note: Any shredder approved for destroying classified documents is also sufficient for use with CUI documents. The Classified Matter Protection and Control Team (cmpc@lanl.gov) approves classified shredders.

3.8.4 *Requirements for Destroying Electronic Media Containing Controlled Unclassified Information (CUI)*

Media that contain CUI may be destroyed by any means approved for destroying classified media.

Users are not required to destroy electronic media that contain CUI. Disks must be overwritten using software such as BCWipe, available through Electronic Software Distribution (ESD), before they are thrown away.

Note: Further questions about this topic should be directed to your Organizational Cyber Security Representative (OCSR).

4.0 RESPONSIBILITIES

4.1 Responsible Line Managers (RLMs)

- Must ensure that controls are in place in their organizations to ensure that CUI is identified, protected, and controlled in accordance with Laboratory procedures.

4.2 Workers

- Must follow all requirements pertaining to the identification, protection, and control of CUI.

5.0 IMPLEMENTATION

Implementation of the requirements in the Telephone section of Section 3.7.5 will take place on September 4, 2012 to allow affected organizations to obtain STEs as needed. During that time, workers are prohibited from discussing UCNI over regular phone lines. The other requirements in this document are effective on the date of issue.

6.0 TRAINING

No formal LANL training is required by this document. An optional Course #22925, *Protecting Unclassified Controlled Nuclear Information-UCNI*, is available.

Additional topics in this document may be covered by courses required by other LANL documents. Informal training, awareness materials, and SME briefings may also be available.

7.0 EXCEPTION OR VARIANCE

To obtain an exception or variance to this document, see the following instructions:

- Managers may request an exception or variance from the IA through the RM.
- At the IA's request, the RM will provide a recommendation or supporting information.
- The IA or designee will provide the requester with a written response and copy the RM.

The requesting organization must maintain the official copy of record of the approved correspondence granting the exception or variance.

8.0 DOCUMENTS AND RECORDS

8.1 Office of Record

The Policy Office is the Laboratory Office of Record for this Institutional Document and maintains the administrative record.

Requirements for creating, approving, and maintaining records or other documents are presented in the main body of this document.

9.0 DEFINITIONS AND ACRONYMS

9.1 Definitions

See LANL *Definition of Terms*.

Controlled Unclassified Information (CUI)—Unclassified information that may be exempt from public release under the FOIA (5 U.S.C. §552 [1966] as amended). CUI is not classified but is subject to legal- or policy-based restrictions on dissemination.

Note: This document describes categories of CUI that are based on and contained in DOE/NNSA directives.

Derivative Classifier (DC)—An individual authorized by the Laboratory Classification Officer (SAFE-1 group leader) to classify documents or materials containing RD, Formerly Restricted Data (FRD), and/or National Security Information (NSI) within his or her programmatic jurisdiction up to the level defined in his or her letter of authorization, using approved classification guidance.

Document—Any record of information, regardless of physical form or characteristics, including, but not limited to, the following:

- All handwritten, printed, or typed matter.
- All painted, drawn, or engraved matter.
- All sound, magnetic, electromechanical or optical recordings.
- All photographic prints, exposed or developed film, and still or motion pictures.
- Automatic information system input, memory, program or output information (e.g., word processor files, e-mail messages) recorded on any medium such as punch cards, tapes, memory (e.g., disks, removable thumb drives), or visual displays.
- All reproductions of the foregoing by any process.

  Note: Review and marking requirements apply to all documents, regardless of format.

Formerly Restricted Data (FRD)—Classified information that the DOE or its predecessor agencies and the Department of Defense have jointly determined (1) to be related primarily to the military utilization of atomic weapons and (2) can be adequately safeguarded in a manner similar to NSI. It is also subject to the restrictions on transmission to other countries and regional defense organizations that apply to RD.

Lawful Permanent Resident—A foreign national who has been authorized to live and work permanently in the US. Evidence of Lawful Permanent Resident status is a plastic encoded document, known officially as the Permanent Resident Card, or green card.

Need to Know—A determination by persons having responsibility for classified or sensitive information or matter that a proposed recipient's access to such classified or sensitive information or matter is necessary in the performance of his or her official or contractual duties of employment.

Official Use Only (OUO)—Information that must be unclassified; have the potential to damage government, commercial, or private interests if disseminated to persons who do not need to know the information to perform their jobs or other DOE-authorized activities; and fall under at least one of seven FOIA exemptions (i.e., Exemptions 3 through 9; information falling under Exemption 1 can never be OUO because it covers information classified by Executive Order).

Reviewing Official—A worker authorized by SAFE-1 to determine, based on UCNI guidelines, if matter under his or her cognizance contains UCNI.

Responsible Line Manager (RLM)—First level manager in the line-management chain who is responsible for security in his or her organization (e.g., division director, group leader, program manager, or office leader). The RLM establishes and manages security initiatives, determines and communicates the desired end-state, allocates resources, assesses performance, and provides methods of accountability. The RLM also actively involves his or her workers in providing feedback and improving the security of their work and workplace.

Restricted Data (RD)—All data concerning design, manufacture, or use of atomic weapons; production of SNM; or use of SNM in the production of energy, except for data declassified or removed from the RD category pursuant to Section 142 of the Atomic Energy Act of 1954, as amended.

Transmittal document—A document containing information about the sender, recipient, and contents of another document being transmitted (usually by electronic means). A fax cover sheet is an example of a transmittal document.

Unclassified Controlled Nuclear Information (UCNI)—Unclassified government information concerning nuclear material, weapons, and components whose dissemination is controlled under Section 148 of the Atomic Energy Act. Specifically, information that has been determined to be UCNI by an UCNI Reviewing Official using DOE-approved UCNI guidelines (42 U.S.C. Chapter 23 §2168 [2008]).

Worker—Any person who performs work at the Laboratory (whether on the Laboratory's DOE-owned, leased, or rental property). Workers include LANS employees, subcontractors, vendors, external organization employees, affiliates, and official visitors.

9.2 Acronyms

See LANL *Acronym Master List*.

ADSS	Associate Director for Security and Safeguards
AT	Applied Technology
CD	Compact Disc
CFR	Code of Federal Regulations
CRADA	Cooperative Research and Development Agreement
CUI	Controlled Unclassified Information
DC	Derivative Classifier
DHS	Department of Homeland Security
DOE	Department of Energy
DOE-NE	Department of Energy Office of Nuclear Energy
DVD	Digital Video Disc
ECI	Export Controlled Information
ESD	Electronic Software Distribution
FOIA	Freedom of Information Act
FRD	Formerly Restricted Data
GSA	General Services Administration
IA	Issuing Authority
LA-CP	Los Alamos-Controlled Publication
LANL	Los Alamos National Laboratory

LANS	Los Alamos National Security, LLC
LPI	LANS Contractor Owned and Proprietary Information
M&O	Management and Operating
NAVSEAINST	Naval Sea Systems Command Instruction
NIST	National Institute of Standards and Technology
NNPI	Naval Nuclear Propulsion Information
NNSA	National Nuclear Security Administration
NRC	Nuclear Regulatory Commission
NSI	National Security Information
OCSR	Organizational Cyber Security Representative
OSTI	Office of Scientific and Technical Information
OUO	Official Use Only
PII	Personal Identifiable Information
RD	Restricted Data
RLM	Responsible Line Manager
RM	Responsible Manager
RO	Responsible Office
ROM	Read Only Memory
RSI	Reactor Safeguards Information
SAFE	Safeguards
SAFE-1	Classification
SME	Subject Matter Expert
SNM	Special Nuclear Material
SSN	Social Security Number
STE	Secure Terminal Equipment
UCNI	Unclassified Controlled Nuclear Information
US	United States

10.0 HISTORY

Revision History		
01/25/09	P204-1, Rev. 0	Initial Issue.
07/15/08	P204-1, Rev. 1	Added clarifying information that Export Controlled Information (ECI) and Applied Technology (AT) information are subcategories of Official Use Only (OUO) information. Reordered the document to reflect this relationship. Added minor clarifications for identifying and properly marking OUO information.
11/19/09	P204-1, Rev. 2	Title changed from "Unclassified Controlled Information to "Controlled Unclassified Information." Added significant new requirements for identifying and handling Personal Identifiable Information (PII). Made changes to the requirements for OUO.

Revision History		
03/02/12	P204-1, Rev. 3	Removed requirement to mark top of Unclassified Controlled Nuclear Information (UCNI) document. Added "Derivative Classifier," "Formerly Restricted Data," and "Restricted Data" to the Definitions. Updated Freedom of Information Act (FOIA) exemptions. Clarified requirement for UCNI transmission over telephone lines. Updated links.

11.0 REFERENCES

Prime Contract:

- 10 CFR 1017, *Identification and Protection of Unclassified Controlled Nuclear Information*
- DOE O 471.1B, *Identification and Protection of Unclassified Controlled Nuclear Information*
- Section 142 of the Atomic Energy Act of 1954, as amended
- 42 U.S.C. Chapter 23 §2168 (2008)
- Clause I-65, DEAR 952.204-70, *Classification/Declassification* (Sept. 1997)
- Clause I-66, DEAR 952.204-71, *Sensitive Foreign Nations Controls* (Apr. 1994)
- Clause I-77, DEAR 970.5204-1, *Counterintelligence* (Dec. 2000)
- Clause I-118, DEAR 952.204-2, *Security* (May 2002)
- Clause I-78, DEAR 970.5204-3, *Access to and Ownership of Records*
- Clause I-121, DEAR 970.5203-1, *Management Controls*
- Clause I-122, DEAR 970.5203-3, *Contractor's Organization* (Dec. 2000)
- Clause I-123, DEAR 970.5204-2, *Laws, Regulations, and DOE Directives* (Dec. 2000)
- H-1, *Redefining the Federal/Contractor Relationship to Improve Management and Performance*
- H-4, *Contractor Assurance System*
- H-6, *Parent Organization's Oversight Plan*
- H-10, *Benchmarking And Standards Management*
- H-11, *Contractor Reinvestment of Cost Efficiencies*
- DOE M 471.3-1, Chg. 1, *Manual for Identifying and Protecting Official Use Only Information*
- DOE O 471.3, Chg. 1, *Identifying and Protecting Official Use Only Information*

11.1 Other References

- NAVSEAINST C5511.32B, *Safeguarding of Naval Nuclear Propulsion Information (NNPI) Naval Sea Systems Command Instruction*
- P202-4, *Security Locks and Keys*
- 5 U.S.C. §552 (1966) as amended
- 22 U.S.C. §2751

- 42 U.S.C. §2077
- 50 U.S.C. §2401
- 10 CFR 810, *Assistance to Foreign Atomic Energy Activities*
- P204-2, *Classified Matter Protection and Control Handbook*
- Electronic Software Distribution
- 10 CFR 73.21, *Requirements for the Protection of Safeguards Information*
- 15 CFR 768-799, *US Department of Commerce Export Administration Regulations*
- 22 CFR 120-130, *US Department of State International Traffic in Arms Regulations*
- P805, *Export Control*
- Office of Scientific and Technical Information (OSTI) Dictionary, Revision 12, DOE Office of Scientific and Technical Information, June 2008

12.0 FORMS

Form 1704, *Certificate of Records Destruction (Unclassified and Classified)*
Form 1756a, *LA-CP Cover—Unclassified Controlled Nuclear Information (UCNI)*
Form 1756b, *LA-CP Cover—UCNI and Official Use Only (OUO) information*
Form 1756c, *LA-CP Cover—Only OUO information*
Form 1756d, *LA-CP Cover—All other unclassified controlled information*
Form 1756e, *LA-CP Cover—Classified information*
Form 1756g, *LA-CP Cover—Export Controlled Information/Official Use Only*

13.0 ATTACHMENTS

There are no attachments associated with this document.

14.0 CONTACT

Classification Group (SAFE-1)
Telephone: (505) 667-5011
E-mail: dgerth@lanl.gov
Website: http://int.lanl.gov/security/classification/